Continuants and some decompositions into squares

Charles Delorme*
Laboratoire de Recherche en Informatique
Université Paris-Sud

Guillermo Pineda-Villavicencio†
Centre for Informatics and Applied Optimization
University of Ballarat

December 21, 2011

Abstract

In 1855 H. J. S. Smith [2] proved Fermat's Two Squares using the notion of palindromic continuants. In his paper Smith constructed a proper representation as a sum of two squares of a prime number p, given a solution of $z^2 + 1 \equiv 0 \pmod{p}$, and vice versa. In this paper we extend Smith's approach to proper representations by sums of two squares in rings of polynomials on fields of characteristic different from 2. Our approach will also work for other representations of integers, such as sums of four squares.

We keep as far as possible the palindromic character of the representations. While our results are likely not new, we believe our extension of Smith's approach is new.

Keywords: Fermat's two squares theorem; four squares theorem; continuant; integer representation.

*cd@lri.fr
†work@guillermo.com.au

1 Introduction

Fermat's Two Squares Theorem, that is

A prime number p is representable by the form $x^2 + y^2$ iff -1 is a quadratic residue modulo p.

has always captivated the mathematical community. Equally captivating are the known proofs of such a theorem; see, for instance, [1, 2, 7, 11, 13]. Among these proofs we were enchanted by Smith's elementary approach [2], which is well within the reach of undergraduates. We remark Smith's proof is very similar to Hermite's [7], Serret's [11], and Brillhart's [1].

Two main ingredients of Smith's proof are the notion of continuant (Definition 2 for arbitrary rings) and the famous Euclidean algorithm (stated for arbitrary Euclidean rings in Table 1).

Let us recall here, for convenience, a definition taken from [8, p.148]

Definition 1 Euclidean rings *are rings R with no zero divisors which are endowed with a Euclidean function* N *from R to the nonnegative integers such that for all $\tau_1, \tau_2 \in R$ with $\tau_1 \neq 0$, there exists $q, r \in R$ such that $\tau_2 = q\tau_1 + r$ and $\mathrm{N}(r) < \mathrm{N}(\tau_1)$.*

Among well-known examples, we are going to use the integers with $\mathrm{N}(u) = |u|$, polynoms over a field with $\mathrm{N}(P) = 2^{\mathrm{degree}(P)}$ and $\mathrm{N}(0) = 0$.

The sequence $(q_1, q_2, \ldots, q_n)$ given by the Euclidean algorithm (Table 1) on τ_1 and τ_2, with τ_1 and τ_2 in R, is called the *continuant representation* of (τ_1, τ_2) as we have the equalities $\tau_1 = [q_1, q_2, \ldots, q_n]h$ (this notation is defined in next paragraph) and $\tau_2 = [q_2, \ldots, q_n]h$ unless $\tau_2 = 0$. If $\tau_2 \neq 0$, then h is a gcd of (τ_1, τ_2), else $h = \tau_1$; in other words $R\tau_1 + R\tau_2 = Rh$, where $R\tau$ denotes the left ideal generated by τ.

Definition 2 (Continuants in arbitrary rings) *Let Q be a sequence of elements $(q_1, q_2, \ldots, q_n)$ of a ring R. We associate to Q an element $[Q]$ of R via the following recurrence formula*

$$[\,] = 1, [q_1] = q_1, [q_1, q_2] = q_1 q_2 + 1, \text{ and}$$
$$[q_1, q_2, \ldots, q_n] = [q_1, \ldots, q_{n-1}]q_n + [q_1, \ldots, q_{n-2}] \quad \text{if } n \geq 3.$$

The value $[Q]$ is called the continuant *of the sequence Q.*

Table 1: Euclidean division

input: Two elements τ_1, τ_2
of a Euclidean ring R
with its Euclidean function N.
output: a gcd of $\tau 1, \tau 2$ followed by
a sequence $(q_1, q_2, \ldots, q_n)$, possibly empty, of elements of R
$n \leftarrow 1$
while $\tau_2 \neq 0$
find q_n, t such that $\tau_1 = q_n \tau_2 + t$ with $\mathrm{N}(t) < \mathrm{N}(\tau_2)$
$n \leftarrow n + 1$
$\tau_1 \leftarrow \tau_2$
$\tau_2 \leftarrow t$
endwhile
return τ_1 followed by $(q_1, q_2, \ldots, q_n)$

Let p be a prime number of the form $4k + 1$. Smith's approach [2] relies on the existence of a palindromic sequence $Q = (q_1, \ldots, q_s, q_s, \ldots, q_1)$ of even length such that $p = [Q]$. He then derives a solution for $z^2 + 1 \equiv 0 \pmod{p}$ with $2 \leq z \leq p/2$, namely $[q_2, \ldots, q_s, q_s, \ldots, q_1]$. On the other hand, from this solution one can retrieve the palindromic sequence by applying the Euclidean algorithm to p and z, and then $p = x^2 + y^2$ where $x = [q_1, \ldots, q_s]$ and $y = [q_1, \ldots, q_{s-1}]$.

Brillhart's optimisation [1] on Smith's construction took full advantage of the palindromic structure of the sequence $(q_1, \ldots, q_{s-1}, q_s, q_s, q_{s-1}, \ldots, q_1)$ given by the Euclidean algorithm on p and z. He noted that the Euclidean algorithm gives the remainders

$$\begin{aligned} r_i &= [q_{i+2}, \ldots, q_{s-1}, q_s, q_s, q_{s-1}, \ldots, q_1] \ (i = 1, \ldots, 2s-1), \text{ and} \\ r_{2s} &= 0 \end{aligned}$$

so, in virtue of Smith's construction, rather than computing the whole sequence we need to obtain

$$\begin{cases} x &= r_{s-1} = [q_s, q_{s-1}, \ldots, q_1] \\ y &= r_s = [q_{s-1}, \ldots, q_1]. \end{cases}$$

In this case, we have $y < x < \sqrt{p}$, Brillhart's stopping criterium.

In this paper we study *proper* representations $x^2 + y^2$ (that is, with x, y coprime) in some Euclidean rings via continuants. In Section 2 we study

some properties of continuants in arbitrary rings. Section 3 is devoted to study proper representations $x^2 + y^2$ in some Euclidean rings. We examine later some representations $x\overline{x} + y\overline{y}$ using rings with an anti-automorphism (Sections 4 and 5), keeping the palindromic (or quasi-palindromic) nature, up to multiplication by units, of the continuant. While the results presented here are not likely new, we believe our presentation is new.

2 Continuants

In this section we derive some properties of continuants from Definition 2, which we will refer to as Continuant Properties.

P–1 The first property is the so-called "Euler's rule" [3, p. 72]: once we have all the products of subsequences of Q obtained by removing disjoint pairs of consecutive elements of Q, the continuant $[Q]$ is given by the sum of all such products. The empty product is 1, as usual.

P–2 If in a ring R we find a unit τ commuting with all q_i's, then

$$[\tau^{-1}q_1, \tau q_2, \ldots, \tau^{(-1)^k}q_k, \ldots, \tau^{(-1)^n}q_n] = \begin{cases} [q_1, \ldots, q_n] & \text{if } n \text{ even} \\ \tau^{-1}[q_1, \ldots, q_n] & \text{if } n \text{ odd} \end{cases}$$

P–3 $[q_1, \ldots, q_n] = [q_1, \ldots, q_{i-1}][q_{i+2}, \ldots, q_n] + [q_1, \ldots, q_i][q_{i+1}, \ldots, q_n]$

To obtain this equality, it suffices to divide the products of subsequences of $Q = (q_1, q_2, \ldots, q_n)$ obtained by removing disjoint pairs of consecutive elements of Q into two groups, depending on whether the pair q_iq_{i+1} $(1 \leq i < n)$ has been removed or not.

P–4 From the previous points follows

$$[-q_h, -q_{h-1}, \ldots, -q_1, 0, q_1, q_2, \ldots, q_n] = \begin{cases} [q_{h+2}, q_{h+3}, \ldots, q_n] & \text{for } 0 \leq h \leq n-2 \\ 1 & \text{if } h = n-1 \\ 0 & \text{if } h = n \end{cases}$$

P–5 $[q_1, \ldots, q_n]$ and $[q_1, \ldots, q_{n-1}]$ are coprime. Note that from the previous points P–3 and P–4 we have more precisely

$$[-q_{n-1}, -q_{n-2}, -q_1, 0][q_1, \ldots, q_n] + [-q_{n-1}, -q_{n-2}, -q_1][q_2, \ldots, q_n] = 1.$$

2.1 Continuants in commutative rings

If the ring R is commutative, then we have some additional properties.

P–6 $[q_1, q_2, \ldots, q_n] = [q_n, \ldots, q_2, q_1]$.

P–7 The continuant $[q_1, \ldots, q_n]$ is the determinant of the tridiagonal $n \times n$ matrix $A = (a_{ij})$ with $a_{i,i} = q_i$ for $1 \leq i \leq n$, $a_{i,i+1} = 1$ and $a_{i+1,i} = -1$ for $1 \leq i < n$.

The following identity due to Lewis Carroll (alias Charles Lutwidge Dodgson) plays an important role in our study of continuants.

Lemma 1 (Lewis Carroll Identity) *Let C be an $n \times n$ matrix in a commutative ring. Let $C_{i_1,\ldots,i_s;j_1,\ldots,j_s}$ denote the matrix obtained from C by omitting the rows $i_1, \ldots, i_s$ and the columns $j_1, \ldots, j_s$. Then*

$$\det(C)\det(C_{i,j;i,j}) = \det(C_{i;i})\det(C_{j;j}) - \det(C_{i;j})\det(C_{j;i})$$

where the determinant of the 0×0 matrix is 1 for convenience.

The use of Lewis Carroll Identity and property P–7 provides more properties.

P–8 $[q_1, q_2, \ldots, q_n][q_2, \ldots, q_{n-1}] = [q_1, \ldots, q_{n-1}][q_2, \ldots, q_n] + (-1)^n$ (when $n \geq 2$).

P–9 In the case of even n with $q_i = q_{n+1-i}$ for $1 \leq i \leq n$, in other words if the sequence is *palindromic*, we see

$$\begin{aligned}
&[q_1, \ldots, q_{n/2}, q_{n/2}, \ldots, q_2]^2 + 1 = \\
&[q_1, \ldots, q_{n/2}, q_{n/2}, \ldots, q_1][q_2, \ldots, q_{n/2}, q_{n/2}, \ldots, q_2] = \\
&([q_1, \ldots, q_{n/2}]^2 + [q_1, \ldots, q_{n/2-1}]^2)([q_2, \ldots, q_{n/2}]^2 + [q_2, \ldots, q_{n/2-1}]^2)
\end{aligned}$$

More properties and proof techniques valid in the commutative case are given in [6, ch. 6.7]

2.2 Quasi-palindromic sequences

Here again the rings are not necessarly commutative.

Definition 3 *An* anti-automorphism *of a ring R is an involution $\tau \mapsto \overline{\tau}$ such that $\overline{\tau+\sigma} = \overline{\tau} + \overline{\sigma}$ and $\overline{\tau\sigma} = \overline{\sigma}\,\overline{\tau}$ for all elements τ, σ of R.*

Definition 4 *Let R be a ring endowed with an anti-automorphism $\tau \mapsto \overline{\tau}$. A* quasi-palindromic *sequence of length n satisfies $q_i = \overline{q_{n+1-i}}$ for $1 \leq i \leq n$; in particular, if n is odd the element $q_{(n+1)/2}$ satisfies $q_{(n+1)/2} = \overline{q_{(n+1)/2}}$.*

We have an obvious relation,

P–10 $[\overline{q_n}, \ldots, \overline{q_1}] = \overline{[q_1, \ldots q_n]}$

and counterparts of the properties P–8 and P–9.

Lemma 2 (Noncommutative Lewis-Carroll-like Identity) *Let $\tau \mapsto \overline{\tau}$ be an anti-automorphism in a ring R, satisfying moreover the conditions*

$$\begin{cases} \tau\overline{\tau} = \overline{\tau}\tau \\ \text{if } \overline{\tau} = \tau \text{ then } \tau \text{ belongs to the centre of } R. \end{cases} \tag{1}$$

Let $(q_1, \ldots q_n)$ be a quasi-palindromic sequence of length $n \geq 2$ in R. The following relation holds

$$\begin{aligned} [q_1, \ldots, q_n][q_2, \ldots, q_{n-1}] &= [q_2, \ldots, q_n][q_1, \ldots, q_{n-1}] + (-1)^n \\ &= [q_1, \ldots, q_{n-1}][q_2, \ldots, q_n] + (-1)^n. \end{aligned}$$

Proof. We proceed by induction on n. Our basic cases are $n = 2, 3$. The result is clearly true for $n = 2$.

For $n = 3$, since q_2 is in the centre of R and q_1 commutes with q_3, from

$$\begin{aligned} [q_1, q_2][q_2, q_3] - 1 &= (q_1q_2 + 1)(q_2q_3 + 1) - 1 \\ &= q_1q_2q_2q_3 + q_1q_2 + q_2q_3 \\ &= q_1q_2q_2q_3 + q_1q_2 + q_2q_3 \end{aligned}$$

we obtain $q_1q_2q_2q_3 + q_1q_2 + q_2q_3 = [q_2, q_3][q_1, q_2] - 1 = [q_1, q_2, q_3]q_2$.

For larger n, write $E = [q_2, \ldots, q_{n-1}]$ and $F = [q_3, \ldots, q_{n-2}]$. Thus, E and F belong to the centre of R, and the following results come from the definition of continuant and Property P–3

$$\begin{aligned}[q_1, \ldots, q_{n-1}][q_2, \ldots, q_n] &= (q_1 E + [q_3, \ldots, q_{n-1}])(Eq_n + [q_2, \ldots, q_{n-2}]) \\ &= q_1 E^2 q_n + q_1 E[q_2, \ldots, q_{n-2}] + [q_3, \ldots, q_{n-1}]Eq_n \\ &+ [q_3, \ldots, q_{n-1}][q_2, \ldots, q_{n-2}]\end{aligned}$$

$$\begin{aligned}[q_1, q_2, \ldots, q_{n-1}, q_n]E &= (q_1[q_2, \ldots, q_{n-1}, q_n] + [q_3, \ldots, q_n])E \\ &= (q_1(Eq_n + [q_2, \ldots, q_{n-2}]) + [q_3, \ldots, q_{n-1}]q_n + F)\, E \\ &= q_1 E q_n E + q_1[q_2, \ldots, q_{n-2}]E + [q_3, \ldots, q_{n-1}]q_n E + FE.\end{aligned}$$

First note that $[q_2, \ldots, q_n][\underline{q_1, \ldots, q_{n-1}}] = [q_1, \ldots, q_{n-1}][q_2, \ldots, q_n]$ because of the equality $[q_1, \ldots, q_{n-1}] = \overline{[q_2, \ldots, q_n]}$.

Since E commutes with the whole R, we have

$$\begin{aligned}q_1 E^2 q_n &= q_1 E q_n E \\ q_1 E[q_2, \ldots, q_{n-2}] &= q_1[q_2, \ldots, q_{n-2}]E, \text{ and} \\ [q_3, \ldots, q_{n-1}]Eq_n &= [q_3, \ldots, q_{n-1}]q_n E\end{aligned}$$

It only remains to check

$$\begin{aligned}EF &= [q_2, \ldots, q_{n-2}][q_3, \ldots, q_{n-1}] + (-1)^n \\ &= [q_3, \ldots, q_{n-1}][q_2, \ldots, q_{n-2}] + (-1)^n\end{aligned}$$

but these equalities follows from the inductive hypothesis. □

Remark 1 *For a quasi-palindromic sequence Q of length $n \geq 3$, we have*

$$\begin{aligned}[q_1, q_2, \ldots, q_{n-1}] &= q_1[q_2, \ldots, q_{n-1}] + [q_3, \ldots, q_{n-1}] \\ &= q_1[q_2, \ldots, q_{n-1}] + \overline{[q_2, \ldots, q_{n-2}]}\end{aligned}$$

3 Proper representations in Euclidean rings

As Smith's approach heavily depends on the existence of a Euclidean-like division algorithm, one may try to extend it to other Euclidean rings R. However, the uniqueness of the continuant representation may be lost. Basically, the uniqueness of the continuant representation boils down to the

uniqueness of the quotients and the remainders in the division algorithm. This uniqueness is achieved only when R is a field or $R = \mathbb{F}[T]$, polynomial algebra over a field $\mathbb{F}$ [9] (considering the degree as the Euclidean function). Note that in $\mathbb{Z}$ we guarantee uniqueness by requiring the remainder to be nonnegative.

3.1 Non-commutative Euclidean rings

We first use continuants to obtain a multiple $z\overline{z} + 1$ of an element m of the form $x\overline{x} + y\overline{y}$, with x, y satisfying $Rx + Ry = R$ and $\tau \mapsto \overline{\tau}$ an anti-automorphism in the ring under consideration.

Theorem 1 *Let R be an Euclidean ring, and let $\tau \mapsto \overline{\tau}$ be an anti-automorphism of R satisfying relations (1). If $m \in R$ admits a* proper *representation $m = x\overline{x} + y\overline{y}$ (that is, with $Rx + Ry = R$), then the equation $z\overline{z} + 1 \in Rm$ admits solutions.*

Furthermore, one of these solutions is equal to $[\overline{q_s}, \ldots, \overline{q_1}, q_1, \ldots, q_{s-1}]$, where $(q_1, q_2, \ldots, q_s)$ is the sequence provided by the Euclidean algorithm on x and y.

Proof. Let (x, y) (with $\mathrm{N}(x) \geq \mathrm{N}(y)$) be a proper representation of m.

If $y = 0$ then x is a unit, so m must be a unit and the ideal $R\tau$ is the whole ring R. Otherwise, the Euclidean algorithm on x and y gives a unit u and a sequence $(q_1, q_2, \ldots, q_s)$ such that $x = [q_1, q_2, \ldots, q_s]u$ and $y = [q_2, \ldots, q_s]u$. Then

$$x\overline{x} = [q_1, \ldots, q_s]u\overline{u}[\overline{q_s}, \ldots, \overline{q_1}], \text{ using Continuant Property P–10}$$
$$x\overline{x} = [\overline{q_s}, \ldots, \overline{q_1}][q_1, \ldots, q_s]u\overline{u}, \text{ since } u\overline{u} \text{ belongs to the centre of } R$$

$$y\overline{y} = [\overline{q_s}, \ldots, \overline{q_2}][q_2, \ldots, q_s]u\overline{u}$$
$$m = x\overline{x} + y\overline{y} = [\overline{q_s}, \ldots, \overline{q_1}, q_1, \ldots, q_s]u\overline{u}, \text{ using Continuant Property P–3}$$

Let $z = [\overline{q_s}, \ldots, \overline{q_1}, q_1, \ldots, q_{s-1}]$, then applying Lemma 2 we obtain

$$z\overline{z} + 1 = (u\overline{u})^{-1}m[\overline{q_{s-1}}, \ldots, \overline{q_1}, q_1, \ldots, q_{s-1}]$$
$$= (u\overline{u})^{-1}[\overline{q_{s-1}}, \ldots, \overline{q_1}, q_1, \ldots, q_{s-1}]m$$
since m is in the center of R

That is, z satisfies $z\overline{z} + 1 \in Rm$, which completes the proof of the theorem. □

3.2 Commutative rings: from x^2+y^2 to z^2+1 and back

In this section we deal with the problem of going from a representation x^2+y^2 of an element m to a multiple z^2+1 of m and back. We begin with a very general remark valid in every commutative ring.

Corollary 1 *In a commutative ring R, if $Rx + Ry = R$ then there exists some $z \in R$ such that $x^2 + y^2$ divides $z^2 + 1$.*

If R is Euclidean, we can explicit z and $(z^2+1)/(x^2+y^2)$ with continuants.

This relation can be interpreted using Lewis-Carroll Identity. The determinant of the tridiagonal matrix A associated to the palindromic sequence $(q_n, \ldots, q_1, q_1, \ldots, q_n)$ (see property P–7 of continuants) is $x^2 + y^2$ with $x = [q_1, \ldots, q_n]$ and $y = [q_2, \ldots, q_n]$ if $n \geq 1$.

Moreover $(x^2 + y^2)([q_1, \ldots q_{n-1}]^2 + [q_2, \ldots q_{n-1}]^2) = z^2 + 1$ where z is the determinant of matrix formed by the $2n-1$ first rows and columns of A (see properties P–8 and P–6).

A natural question is then: if m divides $z^2 + 1$ does there exist x, y such that $m = x^2 + y^2$? But this question is much harder! We now give examples showing that no simple answer is to be expected.

In general we cannot construct a representation $x^2 + y^2$ of an element m from a solution of $z^2 + 1 \equiv 0 \pmod{m}$.

As an illustration, consider the Euclidean domain $\mathbb{F}_2[X]$ of polynomials on the field $\mathbb{F}_2$, where $z^2 + 1$ is a multiple of $m = z + 1$ for any polynomial z, square or not. Recall that in $\mathbb{F}_2[X]$ the squares, and therefore the sums of squares, are exactly the even polynomials (i.e. the coefficient of X^t is null if t is odd). Thus, the converse of Corollary 1 is false in $\mathbb{F}_2[X]$.

Other examples are the ring $\mathbb{Z}[i]$ of Gaussian integers and its quotients by an even integer, since the squares and the sum of squares have an even imaginary part. Thus, no Gaussian integer with an odd imaginary part is a sum of squares, although it obviously divides $0 = i^2 + 1$.

However, there are cases where the answer is positive

Proposition 1 *Let R be a commutative ring. If 2 is invertible and -1 is a square, say $1 + k^2 = 0$, then $x = \left(\frac{x+1}{2}\right)^2 + \left(\frac{x-1}{2k}\right)^2$*

Proposition 2 *Let $R = \mathbb{F}[X]$ be the ring of polynomials over a field $\mathbb{F}$ with characteristic different of 2 such that -1 is a non-square in $\mathbb{F}$.*

If m divides z^2+t^2 with z,t coprime, then m is an associate of some x^2+y^2 with x,y coprime.

Proof. We introduce the extension $\mathbb{G}$ of $\mathbb{F}$ by a square root ω of -1. The ring $\mathbb{G}[X]$ is principal and z^2+t^2 factorises as $(z-\omega t)(z+\omega t)$. The two factors are coprime, since their sum and difference are respectively $2z$ and $2\omega t$, and 2 and ω are units. Introduce $\gcd(m, z+\omega t) = x+\omega y$, then $x-\omega y$ is a gcd of m and $z-\omega t$ owing to the natural automorphism of $\mathbb{G}$. The polynomials $x-\omega y$ and $x+\omega y$ are coprime and both divide m. Thus, m is divisible by $(x-\omega y)(x+\omega y) = x^2+y^2$. On the other hand, m divides $(z-\omega t)(z+\omega t)$. Consequently, $(x-\omega y)(x+\omega y)$ is an associate of m. Since $x-\omega y$ and $x+\omega y$ are coprime, we have x, y are coprime. □

This gives some cases where a reciprocal of the first assertion in Corollary 1 holds.

Proposition 3 *Let m be a non-unit of $\mathbb{F}[X]$ and a divisor of z^2+1 for some $z \in \mathbb{F}[X]$ with $\deg(z) < \deg(m)$.*

If $\mathbb{F}$ is a field of characteristic different from 2, where -1 is a non-square, then continuants provide a method for representing m as a sum of squares.

Specifically, the Euclidean algorithm on m and z gives the unit u and the sequence $(uq_s, u^{-1}q_{s-1}, \ldots, u^{(-1)^{s-1}}q_1, u^{(-1)^s}q_1, \ldots, u^{-1}q_s)$ such that $x = [q_1, \ldots, q_s]$ and $y = [q_2, \ldots, q_s]$.

Proof. Having a divisor m of z^2+1, we already now from Proposition 2 that the degree of m is even. We may assume that $\text{degree}(z) < \text{degree}(m)$ as we may divide z by m.

As $m = (x^2+y^2)u$, the Euclidean algorithm on some x and y will give the unit 1 and a sequence $(q_1, \ldots, q_s)$ such that $x = [q_1, \ldots q_s]$ and $y = [q_2, \ldots, q_s]$. We may also assume $\text{degree}(x) > \text{degree}(y)$, otherwise, if $x = \lambda y + z$ with λ a unit and z of degree smaller than the degree of x and y, then $m = (((1+\lambda^2)y + \lambda z)^2 + z^2)\,\frac{u}{1+\lambda^2}$. As a result we consider only the case where all q_i's have degree at least 1.

We then apply the Euclidean algorithm (Table 1) to m and z, and obtain, by virtue of the uniqueness of division in polynomials, a sequence whose last non-null remainder is u. Consequently, $m/u = x^2+y^2$ (see Property P–2 of continuants). □

Below we illustrate this proposition through some examples.

First take $m = 2X^4-2X^3+3X^2-2X+1$, then m divides $(2X^3+X)^2+1$. The Euclidean divisions give successively

$$\begin{aligned} 2X^4 - 2X^3 + 3X^2 - 2X + 1 &= (2X^3 + X)(X - 1) + 2X^2 - X + 1 \\ 2X^3 + X &= (2X^2 - X + 1)(X + 1/2) + (X/2 - 1/2) \\ 2X^2 - X + 1 &= (X/2 - 1/2)(4X + 2) + 2 \\ X/2 - 1/2 &= 2(X/4 - 1/4). \end{aligned}$$

Here we have $m/2 = [2\cdot(X-1)/2, 2^{-1}\cdot(2X+1), 2\cdot(2X+1), 2^{-1}\cdot(X-1)/2]$ with $u = 2$, which gives $m/2 = (X^2 - X/2 + 1/2)^2 + (X/2 - 1/2)^2 = x^2 + y^2$. Since 2 is also a sum of two squares, we obtain $m = (x + y)^2 + (x - y)^2 = X^4 + (X^2 - X + 1)^2$.

We find other examples among the cyclotomic polynomials. The cyclotomic polynomial $\Phi_{4n} \in \mathbb{Q}[X]$ divides $X^{2n}+1$. Thus Φ_{4n} is, up to a constant, a sum of two squares. Since $\Phi_{4n}(0) = 1$, the constant can be chosen equal to 1. For an odd prime p, it is easy to check

$$\Phi_{4p}(X) = \sum_{k=0}^{p-1}(-1)^k X^{2k} = \left(\sum_{k=0}^{(p-1)/2}(-1)^k X^{2k}\right)^2 + \left(X\sum_{k=0}^{(p-3)/2}(-1)^k X^{2k}\right)^2$$

For the small composite odd number 15, the computation gives

$$\begin{aligned} \Phi_{60}(X) &= X^{16} + X^{14} - X^{10} - X^8 - X^6 + X^2 + 1 \\ &= [X, X, X^3 - X, -X, -X, X, X, -X, -X, X^3 - X, X, X] \\ X^{15} &= [X, X^3 - X, -X, -X, X, X, -X, -X, X^3 - X, X, X] \\ x &= [X, -X, -X, X^3 - X, X, X] \\ &= X^8 - X^4 + 1 \\ y &= [-X, -X, X^3 - X, X, X] \\ &= X^7 + X^5 - X^3 - X \\ \Phi_{60}(X) &= x^2 + y^2 \end{aligned}$$

At this stage the following remark is important.

Remark 2 *If a polynomial with integer coefficients is the sum of squares of two polynomials with rational coefficients, it is also the sum of squares of two polynomials with integer coefficients*

For example, we see that $50X^2+14X+1=(5X+3/5)^2+(5X+4/5)^2$, but it is also $X^2+(7X+1)^2$.

A proof was given by Gjergji Zaimi [12]. Another proof can be seen in [4, Sec. 5].

Remark 3 (Algorithmic considerations) *To accelerate the computation in Proposition 3, we can resort to Brillhart's [1] optimisation and stop when we first encounter a remainder r_{s-1} with degree at most* $\mathrm{degree}(m)/2$. *This will be the $(s-1)$-th remainder. In this context*

$$x=\begin{cases} r_{s-1} & \text{for odd } s \\ u^{-1}r_{s-1} & \text{for even } s \end{cases} \qquad y=\begin{cases} [uq_s,u^{-1}q_{s-1},\dots,u^{(-1)^{s-2}}q_2] & \text{for odd } s \\ u^{-1}[uq_s,u^{-1}q_{s-1},\dots,u^{(-1)^{s-2}}q_2] & \text{for even } s \end{cases}$$

This observation follows from dividing $m/u=[q_s,\dots,q_1,q_1,\dots,q_s]$ by $z=[q_{s-1},\dots,q_1,q_1,\dots,q_s]$ using continuant properties.

4 Four squares theorem

We slightly generalise the formula for products of sums of four squares; see [10, p.135] (this was already known to Euler, see [5, p. 277]).

Lemma 3 (Product formula) *Let R be a commutative ring endowed with an anti-automorphism. Let x,y,z,u be elements of R. Then*

$$(x\overline{x}+y\overline{y})(z\overline{z}+u\overline{u})=(xz-y\overline{u})(\overline{xz-y\overline{u}})+(xu+y\overline{z})(\overline{xu+y\overline{z}})$$

Proof. This can be seen by looking at the determinants in the equality

$$\begin{bmatrix} x & y \\ -\overline{y} & \overline{x} \end{bmatrix}\begin{bmatrix} z & u \\ -\overline{u} & \overline{z} \end{bmatrix}=\begin{bmatrix} x & y \\ -\overline{y} & \overline{x} \end{bmatrix}\begin{bmatrix} xz-y\overline{u} & xu+y\overline{z} \\ -\overline{xu+y\overline{z}} & \overline{xz-y\overline{u}} \end{bmatrix}$$

□

The four squares product formula is the application of the lemma 3 to the case where R is the ring of Gaussian integers, with its conjugation.

This product formula allows to reduce the proof of the four squares theorem to the case of primes.

We recall that in $\mathbb{Z}/p\mathbb{Z}$ the element -1 is either a square or a sum of two squares; see [10, p.133] (this also was known to Euler [5, p. 279]). Thus, it suffices to prove that if a positive number m divides $z\overline{z}+1$ with z being

a Gaussian integer, then m is also $x\overline{x} + y\overline{y}$ with x, y both being Gaussian integers.

By reducing z modulo m, we may assume $|z| \leq m/\sqrt{2}$, and thus $z\overline{z}+1 < m^2$ (if $m = 2$, a parity argument shows the inequality remains valid). Here $|z|$ denotes the *complex norm* of z.

Then, we have a succession of s equalities $m_i m_{i+1} = z_i\overline{z_i} + 1$ and $z_i = q_{i+1}m_{i+1}+z_{i+1}$, where the sequence of positive integers $m = m_0, m_1, \ldots, m_s = 1$ is decreasing. At the end we have $m_{s-1}m_s = z_{s-1}\overline{z_{s-1}} + 1$ and $q_s = z_{s-1}$.

Now the quasi-palindromic sequence $Q = (q_1, \overline{q_2}, \ldots, q_2, \overline{q_1})$, where the central pair is $q_s, \overline{q_s}$ if s is odd and $\overline{q_s}, q_s$ if s is even, satisfies $[Q] = m$. Thus, we have a representation of $m = x\overline{x} + y\overline{y}$ with x and y being the continuants of the sequences formed by the first s terms and first $s-1$ terms of Q, respectively. The alternation of quotients and their conjugates is justified by Remark 1.

Consider the following example, where $m_0 = 431$ and $z_0 = 54 + 10i$.

$$\begin{aligned}
431 \cdot 7 = (54 + 10i)(54 - 10i) + 1 &\rightarrow 54 + 10i = (8 + i)7 + (-2 + 3i) \\
7 \cdot 2 = (-2 + 3i)(-2 - 3i) + 1 &\rightarrow -2 + 3i = (-1 + i)2 + i \\
2 \cdot 1 = (i)(-i) + 1 &\rightarrow i = i \cdot 1
\end{aligned}$$

Hence $Q = (q_1, q_2, q_3) = (8 + i, -1 + i, i)$ and

$$\begin{aligned}
431 &= [8 + i, -1 - i, i, -i, -1 + i, 8 - i] \\
&= |[8 + i, -1 - i, i]|^2 + |[8 + i, -1 - i]|^2 = |17 - 5i|^2 + |-6 - 9i|^2 \\
&= 17^2 + 5^2 + 6^2 + 9^2
\end{aligned}$$

5 Some forms representing integers

Using the techniques of Section 4 we may build other forms representing all positive integers. One such form is $x^2 - xy + y^2 + z^2 - zu + u^2$.

Proposition 4 *Each positive integer has the form $x^2-xy+y^2+z^2-zu+u^2$ with x, y, z, u integers.*

Proof. We note that $v^2 - vw + w^2$ is the norm of $v + wj$ in the ring of Eisenstein integers where $j = \exp(2i\pi/3)$. The same arguments as in Section 4 reduce the task to primes and prove that each prime is either of the form $z\overline{z}$ or divides some $z\overline{z} + 1$.

Now, if an integer m divides $z\overline{z}+1$, the division process provides an deterministic algorithm to find a representation $m = x\overline{x} + y\overline{y}$. Here again we reduce z modulo m and assume $z\overline{z} \leq 3m^2/4$. Thus, we only have to be careful if $m_{s-1} = 2$ to avoid the trap $2 \cdot 2 = (1-j)(1-\overline{j})+1$ by choosing a convenient quotient q_{s-1}. □

Consider the following example where we try to represent $m_0 = 40$. We note $80 = 40 \cdot 2 = (7-3j)(7-3\overline{j})+1$. With the quotient $q_1 = 3-j$ we would get $2 \cdot 2 = (1-j)(1-\overline{j})+1$. However, with the quotient $q_1 = 3-2j$, we get $2 \cdot 1 = (1+j)(1+\overline{j})+1$ and $q_2 = 1+j$. Hence

$$\begin{aligned} 40 &= [3-2j, 1+\overline{j}][7-3\overline{j}, 1+j] + [3-2j][3-2\overline{j}] \\ &= (-1-5j)(-1-5\overline{j}) + (3-2j)(3-2\overline{j}) \\ &= 5^2 - 5 \cdot 1 + 1^2 + 3^2 + 3 \cdot 2 + 2^2 \\ &= 21 + 19. \end{aligned}$$

Corollary 2 *Every positive integer has the form $x^2+3y^2+z^2+3u^2$.*

Proof. By Proposition 4 we only need to prove that $x^2 - xy + y^2$ has the form $3p^2 + q^2$. Indeed,

- If x is even, say $x = 2t$, then $x^2 - xy + y^2 = 4t^2 - 2ty + y^2 = 3t^2 + (y-t)^2$
- If y is even, say $y = 2t$, then $x^2 - xy + y^2 = 3t^2 + (x-t)^2$
- If x and y are both odd, then $x^2 - xy + y^2 = ((x+y)/2)^2 + 3((y-x)/2)^2$

□

Proposition 5 *Each integer has the form $x^2 - 3y^2 + z^2 - 3u^2$.*

Proof. This follows reasoning as in Proposition 4. The necessary ring is $\mathbb{Z}[\sqrt{3}]$ endowed with its natural anti-automorphism. □

In the following example we try to represent 19 and -19, noticing that $19 \cdot 2 = 7^2 - 3 \cdot 2^2 + 1$.

$$\begin{aligned} 19 \cdot 2 &= (7+\sqrt{3})(7-\sqrt{3})+1 \\ & \qquad\qquad q_1 = 3+\sqrt{3} \\ 2 \cdot 1 &= (1+0\sqrt{3})(1-0\sqrt{3})+1 \\ & \qquad\qquad q_2 = 1+0\sqrt{3}. \end{aligned}$$

Hence

$$\begin{aligned}19 &= [3+\sqrt{3}, 1-0\sqrt{3}][3-\sqrt{3}, 1+0\sqrt{3}] + [3+\sqrt{3}][3-\sqrt{3}] \\ &= (4+\sqrt{3})(4-\sqrt{3}) + (3+\sqrt{3})(3-\sqrt{3}) \\ &= 16-3+9-3.\end{aligned}$$

Then, to represent -19, we use $-1 = 1\cdot 1 + (1+\sqrt{3})(1-\sqrt{3})$ and the product formula (Lemma 3) to get

$$\begin{aligned}-19 &= ((4+\sqrt{3})(1+\sqrt{3}) + (3+\sqrt{3}))\overline{(4+\sqrt{3})(1+\sqrt{3}) + (3+\sqrt{3})} \\ &\quad + ((4+\sqrt{3}) - (3+\sqrt{3})(1-\sqrt{3}))\overline{(4+\sqrt{3}) - (3+\sqrt{3})(1-\sqrt{3})} \\ &= (10+6\sqrt{3})(10-6\sqrt{3}) + (4+3\sqrt{3})(4-3\sqrt{3}) = -8-11.\end{aligned}$$

Remark 4 *We have proved the existence of decompositions of positive numbers as sums of two norms of Gaussian integers or Eisenstein integers. The number of representations of positive numbers by these forms are given by Jacobi's theorem [?, Theorem 9.5] and Liouville's theorem [?, Theorem 17.3], respectively.*

References

[1] J. Brillhart, *Note on representing a prime as a sum of two squares*, Mathematics of Computation **26** (1972), 1011–1013.

[2] F. W. Clarke, W. N. Everitt, L. L. Littlejohn, and S. J. R. Vorster, *H. J. S. Smith and the Fermat two squares theorem*, The American Mathematical Monthly **106** (1999), no. 7, 652–665, doi:10.2307/2589495.

[3] H. Davenport, *The higher arithmetic-An introduction to the theory of numbers*, 8th ed., Cambridge University Press, Cambridge, 2008, Editing and additional material by J. H. Davenport.

[4] H. Davenport, D. J. Lewis, and A. Schinzel, *Polynomials of certain special types*, Acta arithmetica **IX** (1964), 107–116.

[5] L. E. Dickson, *History of the theory of numbers, Vol. II*, Chelsea Publishing Company, New York, 1971.

[6] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete mathematics: a foundation for computer science*, 2nd ed., Addison-Wesley, New York, 1994.

[7] C. Hermite, *Note au sujet de l'article précédent*, Journal de Mathématiques Pures et Appliquées **5** (1848), 15.

[8] N. Jacobson, *Basic algebra I*, 2nd ed., W. H. Freeman and Company, New York, 1985.

[9] M. A. Jodeit, Jr., *Uniqueness in the division algorithm*, The American Mathematical Monthly **74** (1967), 835–836.

[10] W. L. LeVeque, *Topics in number theory I*, Addison-Wesley Publishing Company, Cambdridge, Mass., 1956.

[11] J. A. Serret, *Sur un théorème relatif aux nombres entiers*, Journal de Mathématiques Pures et Appliquées **5** (1848), 12–14.

[12] G. Zaimi (`http://mathoverflow.net/users/2384/`), *About integer polynomials which are sums of squares of rational polynomials*, Mathoverflow, `http://mathoverflow.net/questions/82046/`, accessed Dec 16 2011.

[13] D. Zagier, *A one-sentence proof that every prime* $p \equiv 1 \pmod 4$ *is a sum of two squares*, The American Mathematical Monthly **97** (1990), no. 2, 144, doi:10.2307/2323918.